

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Fredrik Lindholm

§  
§  
§  
§  
§  
§

Group Art Unit: 2436

Application No 10/552,955

Examiner: Nguyen, Trong H

Filed: 10/14/2005

Confirmation No: 2497

Attorney Docket No: P18053-US1

Customer No.: 27045

For: Authentication Method

**Via EFS-Web**

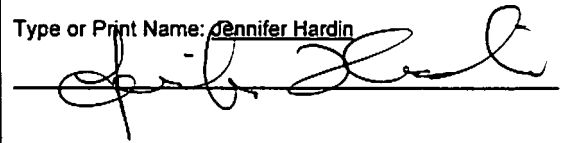
Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313.1450

**CERTIFICATE OF TRANSMISSION BY EFS-WEB**

Date of Transmission: \_\_\_ March 4, 2010

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Jennifer Hardin



**APPEAL BRIEF SUBMITTED UNDER 35 U.S.C. §134**

This Appeal Brief is submitted to appeal the decision of the Primary Examiner set forth in Final Official Action dated August 3, 2009, and the Advisory Action dated November 3, 2009, finally rejecting claims 1-5, 7-11, 13-29, 31, 32 and 34-45, and maintaining an objection to claims 6 and 30.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2) that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1379.

**Real Party in Interest**

The real party in interest, by assignment, is: Telefonaktiebolaget LM Ericsson (publ)  
SE-164 83  
Stockholm, Sweden

### **Related Appeals and Interferences**

None.

### **Status of Claims**

Claims 12, 33, 46 and 47 were previously cancelled and are not appealed. Claims 1-11, 13-32 and 34-45 remain pending; claims 1-5, 7-11, 13-29, 31, 32 and 34-45 stand rejected under 35 U.S.C. §103(a), and claims 6 and 30 stand objected to for an alleged informality.

### **Status of Amendments**

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

### **Grounds of Rejection to be Reviewed on Appeal**

- 1.) Whether claims 6 and 30 include terminology that lacks antecedent basis;
- 2.) Whether claims 1, 10-11, 13-15, 18, 21, 25, 32, 34, 37, 39, 41 and 45 are patentable over Brainard, *et al.* (U.S. Patent No. 7,363,494) in view of Schutzer (U.S. Patent Publication No. 2002/0053035) and Kaufman, *et al.* (U.S. Patent No. 5,491,752);
- 3.) Whether claims 2, 26 and 42 are patentable over Brainard, Schutzer, Kaufman and Uskela (U.S. Patent No. 6,721,886);
- 4.) Whether claims 3, 5, 6, 27, 29, 30 and 43 are patentable over Brainard, Schutzer, Kaufman and Hauser, *et al.* (U.S. Patent No. 5,778,065);
- 5.) Whether claims 4 and 28 are patentable over Brainard, Schutzer, Kaufman, Hauser and Aiello, *et al.* (U.S. Patent No. 6,397,329);
- 6.) Whether claims 7, 8, 31 and 44 are patentable over Brainard, Schutzer, Kaufman, Hauser and Matsumoto (U.S. Patent No. 6,215,877);
- 7.) Whether claim 9 is patentable over Brainard, Schutzer, Kaufman, Hauser, Matsumoto and Gunter, *et al.* (U.S. Patent No. 6,885,388);
- 8.) Whether claims 16, 17, 23, 35, 36 and 40 are patentable over Brainard, Schutzer, Kaufman and Jackson, *et al.* (U.S. Patent No. 4,980,542);

- 9.) Whether claims 19, 20, 24 and 38 are patentable over Brainard, Schutzer, Kaufman and MacKenzie (U.S. Patent No. 7,076,656); and,
- 10.) Whether claim 22 is patentable over Brainard, Schutzer, Kaufman, Hauser and McDowell, *et al.* (U.S. Patent No. 6,668,167)

### Arguments

**1.) Claims 6 and 30 do not include terminology that lacks antecedent basis**

In the Final Office Action dated August 3, 2009, the Examiner objected to claims 6 and 30, stating that "the group" lacks antecedent basis. In Applicant's response, each of those claims was amended to change "the group" to "the group consisting of," following the conventional Markush group claiming structure. In the Advisory Action dated November 3, 2009, the Examiner did not indicate that such amendment overcame the prior objection; the Advisory Action, however, failed to indicate why the Examiner was maintaining the objection. It is requested that the Examiner either withdraw the objection or state the basis for the maintenance of such objection in an answer to this appeal; for purposes of appeal, however, Applicant will concede that those claims stand or fall with the independent claims from which they depend.

**2.) Claims 1, 10-11, 13-15, 18, 21, 25, 32, 34, 37, 39, 41 and 45 are patentable over Brainard, *et al.* (U.S. Patent No. 7,363,494) in view of Schutzer (U.S. Patent Publication No. 2002/0053035) and Kaufman, *et al.* (U.S. Patent No. 5,491,752)**

The Examiner has maintained the rejection of claims 1, 10-15, 18, 21, 25, 32-34, 37, 39, 41, 45-46, and 47 as being unpatentable over Brainard, *et al.* (U.S. Patent No. 7,363,494) in view of Schutzer (U.S. Patent Publication No. 2002/0053035). The Applicant traverses the rejections.

First, it is important to note that the Examiner first rejected independent claims 1, 25 and 42 only over Brainard in view of Schutzer (see Office Action dated November 3, 2008). In a response to that office action, the Applicant amended claims 1, 25 and 42 to include the subject matter of dependent claims 12, 33 and 46, respectively, which were then cancelled. Accordingly, the Applicant addressed the rejections of claims 1, 25 and

41 in view of the Examiner's stated reasons for rejection of claims 12, 33 and 36 (see response to office action filed April 3, 2009). In the next "final" office action, dated August 3, 2009, the Examiner responded to Applicant's arguments, stating that he disagreed with Applicant's arguments and asserting additional reasons why Schutzer taught certain claim limitations. (See "Response to Arguments;" Final Office Action dated August 3, 2009). The Examiner, however, added a new reference (Kaufman) to his stated basis of rejection, and stated that "Applicants' amendment necessitated the new ground(s) of rejection." The claim amendments made in the Applicant's response to the first office action, however, were to incorporate the subject matter of dependent claims into independent claims. Therefore, no new matter was added to the independent claims and, therefore, the finality of that office action was improper. In response to the "final" office action, the Applicant presented additional arguments directed to why the combination of Brainard and Schutz did not render the claimed invention obvious. The Applicant did not specifically address the additional asserted teachings of Kaufman because the Examiner's response first indicated that he found Applicant's arguments "not persuasive" and, through oversight, it was not seen that the Examiner had subsequently added the Kaufman reference to his subsequent stated bases for rejection. The Applicant presents hereinafter the arguments previously presented with respect to the teachings of Brainard and Schutzer, and further arguments as to why Kaufman fails to overcome the deficiencies in those references.

Claim 1 recites:

1. A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of:
  - assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;
  - determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;
    - determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,
    - creating, at the first unit, the check token for the second unit based on the token secret and the password;
    - sending the check token to the second unit; and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first device is authenticated if said check token is the same as said authentication token of said second unit. (emphasis added)

The claimed invention is characterized by individual *authentication* tokens, **assigned to units in a group of at least two units associated with a common password**, that are irreversibly determined by a password. A password inputted by a user of a first unit and an authentication token of the first unit are used to determine a *check* token for a second unit. This is accomplished by first determining, at the first unit, a token secret using the authentication token of the first unit and the inputted password; the *check* token for the second unit is then created based on the token secret and the password. The *check* token is then sent to the second unit where it is compared with the *authentication* token of the second unit; if they are the same, then the user of the first device is considered authenticated. The claimed combination of elements and functions is neither taught, nor suggested, by Brainard or Schutzer, either alone or in combination.

The authentication system taught by Brainard is a conventional client-server, or monolithic, authentication system. In contrast, the Applicant's invention is directed to a distributed solution; any device can authenticate itself against any other device in the system. According to the teachings of Brainard, a user, or a group of users, can be authenticated against a central server, but they cannot be authenticated directly against other member users/devices. Using Applicants' invention, however, **a common password associated with a group of units allows any unit to be authenticated against another unit that is a member of a group without the need for a common authentication server**, such as verification computer 450 taught by Brainard.

In Applicant's response filed on April 3, 2009 to the first, non-final office action dated November 3, 2008, the Applicant amended independent claims 1, 25 and 41 to include the subject matter of claims 12, 33 and 46, respectively, which were then cancelled. Accordingly, the Applicant addressed the rejections of claims 1, 25 and 41 in view of the Examiner's stated reasons for rejection of claims 12, 33 and 36. Claim 1, as amended to include the limitations of claim 12, recites:

1. A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of;  
    assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;  
    determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;  
    determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,  
    creating, at the first unit, the check token for the second unit based on the token secret and the password;  
    sending the check token to the second unit; and,  
    comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first device is authenticated if said check token is the same as said authentication token of said second unit. (emphasis added)

As described *supra*, the claimed invention is characterized by individual **authentication** tokens, assigned to units in a group of at least two units associated with a common password, that are irreversibly determined by a password. A password inputted by a user of a first unit and an authentication token of the first unit are used to determine a **check** token for a second unit. This is accomplished by first determining, at the first unit, a token secret using the authentication token of the first unit and the inputted password; the **check** token for the second unit is then created based on the token secret and the password. The **check** token is then sent to the second unit where it is compared with the **authentication** token of the second unit; if they are the same, then the user of the first device is considered authenticated. The claimed combination of elements and functions is neither taught, nor suggested, by Brainard or Schutzer, either alone or in combination.

The Examiner's stated basis for rejection relied on an incorrect interpretation that "**check** token will be considered to be determined based on the password only;" rather, it is the individual authentication tokens of each unit in a group which are irreversibly determined by a common password. The authentication system taught by Brainard is a conventional client-server, or monolithic, authentication system. In contrast, the

Applicant's invention is directed to a distributed solution; any device can authenticate itself against any other device in the system. According to the teachings of Brainard, a user, or a group of users, can be authenticated against a central server, but they cannot be authenticated directly against other member users/devices. Using Applicants' invention, however, a common password associated with a group of units allows any unit to be authenticated against another unit that is a member of a group without the need for a common authentication server, such as verification computer 450 taught by Brainard.

Furthermore, as acknowledged by the Examiner, Brainard fails to disclose assigning individual authentication tokens to the respective units in a group. To overcome that deficiency, the Examiner looked to the teachings of Schutzer. The Examiner stated that Schutzer teaches providing an authentication token to a user during a registration process. Schutzer does not, however, teach assigning *individual* (i.e., unique) authentication tokens to the respective units in a group based on a password such that each authentication token is irreversibly determined by the password. Therefore, Schutzer fails to overcome the deficiencies in the teachings of Brainard.

In responding to the foregoing arguments in the final office action dated August 3, 2009, the Examiner argued that:

Although, Schutzer was originally relied upon to show assigning individual authentication tokens to respective units in a group, **Schutzer also discloses assigning individual (i.e. unique) authentication tokens to the respective units in a group** based on a password such that each authentication token is irreversibly determined by the password on pars. 0010 or 0024-0025. (emphasis added)

As previously acknowledged by the Examiner, Brainard fails to disclose assigning individual authentication tokens to the respective units in a group. To overcome that deficiency, the Examiner looked to the teachings of Schutzer. Schutzer does not, however, teach individual authentication tokens **assigned to units in a group of at least two units associated with a common password**. Thus, Schutzer fails to overcome the deficiencies in the teachings of Brainard and, therefore, claim 1 is not obvious over Brainard in view of Schutzer.

As noted *supra*, although the Examiner dismissed Applicant's arguments traversing the claim rejections in view of Schutzer and Brainard in the final office action, he *added* Kaufman as a reference. In relying on Kaufman, however, the Examiner did not point to any teaching of the elements that the Applicant had argued were not taught by Schutzer and Brainard (as presented *supra*), but provided only general references to teachings in Kaufman to a "check token" and a "token secret." With respect to a "check token," the Examiner refers to a "transmission code," which Kaufman states is computed based upon a password and a token. The Examiner, however, doesn't provide any support for how that relates to the teachings of Brainard and Schutzer to render claim 1 obvious. Similarly, with respect to a "token secret," the Examiner simply correlates it to a "password | token or hash (password | token)," without any support for how that relates to the teachings of Brainard and Schutzer to render claim 1 obvious. It appears that the Examiner merely added Kaufman as a reference to establish a new ground of rejection necessitated by Applicant's claim amendments in order to make the office action "final." As noted *supra*, however, the finality of the office action was improper because the claim amendments only incorporated subject matter from dependent claims into the pending independent claims. In any case, however, the Examiner has not established a *prima facie* case of how Kaufman, added to the teachings of Schutzer and Brainard, renders claim 1 obvious.

For the foregoing reasons, claim 1 is not obvious over Schutzer in view of Brainard and Kaufman. Whereas independent claims 25 and 41 recite limitations analogous to those of claim 1, they are also not obvious in view of Schutzer and Brainard, or further in view of Kaufman. Furthermore, whereas claims 10-11, 13-15, 18 and 21 are dependent from claim 1; claims 32, 34, 37 and 39 are dependent from claim 25; and claim 45 is dependent from claim 41, and include the limitations of their respective base claims, they are also not obvious over those references.

**3.) Claims 2, 26 and 42 are patentable over Brainard, Schutzer, Kaufman and Uskela (U.S. Patent No. 6,721,886)**

The Examiner has rejected claims 2, 26 and 42 as being unpatentable over Brainard, Schutzer, Kaufman and Uskela (U.S. Patent No. 6,721.886). As established



*supra*, however, independent claims 1, 25 and 41 are not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Uskela that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claims 1, 25 and 41 would not be obvious in further view of Uskela. Therefore, whereas claims 2, 26 and 42 are dependent from claims 1, 25 and 41, respectively, and include the limitations thereof, they are also not obvious.

**4.) Claims 3, 5, 6, 27, 29, 30 and 43 are patentable over Brainard, Schutzer, Kaufman and Hauser, *et al.* (U.S. Patent No. 5,778,065)**

The Examiner has rejected claims 3, 5, 6, 27, 29, 30 and 43 as unpatentable over Brainard, Schutzer, Kaufman and Hauser, *et al.* (U.S. Patent No. 5,778,065). As established *supra*, however, independent claims 1, 25 and 41 are not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Hauser that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claims 1, 25 and 41 would not be obvious in further view of Hauser. Therefore, whereas claims 3, 5, 6 are dependent from claim 1; claims 27, 29 and 30 are dependent from claim 25; and claim 43 is dependent from claim 41, and include the limitations thereof, they are also not obvious.

**5.) Claims 4 and 28 are patentable over Brainard, Schutzer, Kaufman, Hauser and Aiello, *et al.* (U.S. Patent No. 6,397,329)**

The Examiner has rejected claims 4 and 28 as unpatentable over Brainard, Schutzer, Kaufman, Hauser and Aiello, *et al.* (U.S. Patent No. 6,397,329). As established *supra*, however, independent claims 1 and 25 are not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Aiello that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claims 1 and 25 would not be obvious in further view of Aiello. Therefore, whereas claim 4 is dependent from claim 1 and claim 28 is dependent from claim 25, and include the limitations of thereof, they are also not obvious.

**6.) Claims 7, 8, 31 and 44 are patentable over Brainard, Schutzer, Kaufman, Hauser and Matsumoto (U.S. Patent No. 6,215,877)**

The Examiner has rejected claims 7, 8, 31 and 44 as unpatentable over Brainard, Schutzer, Kaufman, Hauser and Matsumoto (U.S. Patent No. 6,215,877). As established *supra*, however, independent claims 1, 25 and 41 are not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Hauser or Matsumoto that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claims 1, 25 and 41 would not be obvious in further view of those references. Therefore, whereas claims 7 and 8 are dependent from claim 1, claim 31 is dependent from claim 25, and claim 44 is dependent from claim 41, and include the limitations thereof, they are also not obvious.

**7.) Claim 9 is patentable over Brainard, Schutzer, Kaufman, Hauser, Matsumoto and Gunter, *et al.* (U.S. Patent No. 6,885,388)**

The Examiner has rejected claim 9 as unpatentable over Brainard, Schutzer, Kaufman, Hauser, Matsumoto and Gunter, *et al.* (U.S. Patent No. 6,885,388). As established *supra*, however, independent claim 1 is not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Hauser, Matsumoto or Gunter that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claim 1 would not be obvious in further view of that reference. Therefore, whereas claim 9 is dependent from claim 1, and includes the limitations thereof, it is also not obvious.

**8.) Claims 16, 17, 23, 35, 36 and 40 are patentable over Brainard, Schutzer, Kaufman and Jackson, *et al.* (U.S. Patent No. 4,980,542)**

The Examiner has rejected claims 16, 17, 23, 35, 36 and 40 as unpatentable over Brainard, Schutzer, Kaufman, and Jackson, *et al.* (U.S. Patent No. 4,980,542). As established *supra*, however, independent claims 1, 25 and 41 are not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Jackson that would overcome the deficiencies in Brainard, Schutzer and Kaufman and,

therefore, claims 1, 25 and 41 would not be obvious in further view of that reference. Therefore, whereas claims 16, 17 and 23 are dependent from claim 1, and claims 35, 36 and 40 are dependent from claim 25, and includes the limitations thereof, they are also not obvious.

**9.) Claims 19, 20, 24 and 38 are patentable over Brainard, Schutzer, Kaufman and MacKenzie (U.S. Patent No. 7,076,656)**

The Examiner has rejected claims 19, 20, 24 and 38 as unpatentable over Brainard, Schutzer, Kaufman, and MacKenzie (U.S. Patent No. 7,076,656). As established *supra*, however, independent claims 1 and 25 are not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in MacKenzie that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claims 1 and 25 would not be obvious in further view of that reference. Therefore, whereas claims 19, 20 and 24 are dependent from claim 1, and claim 38 is dependent from claim 25, and includes the limitations thereof, they are also not obvious.

**10.) Claim 22 is patentable over Brainard, Schutzer, Kaufman, Hauser and McDowell, et al. (U.S. Patent No. 6,668,167)**

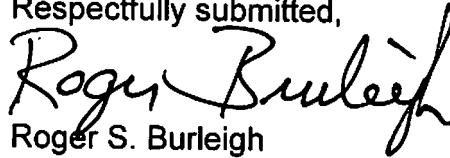
The Examiner has rejected claim 22 as unpatentable over Brainard, Schutzer, Kaufman, Hauser, and McDowell, *et al.* (U.S. Patent No. 6,668,167). As established *supra*, however, independent claim 1 is not obvious over Brainard, Schutzer and Kaufman. The Examiner has not pointed to any teaching in Hauser, or McDowell that would overcome the deficiencies in Brainard, Schutzer and Kaufman and, therefore, claim 1 would not be obvious in further view of that reference. Therefore, whereas claim 22 is dependent from claim 1, and includes the limitations thereof, it is also not obvious.

\* \* \*

**CONCLUSION**

Claims 1-11, 13-32 and 34-45 currently are patentable over the cited art, and the Applicant requests that the Examiner's rejections thereof be reversed and the application be remanded for further prosecution.

Respectfully submitted,



Roger S. Burleigh  
Registration No. 40,542  
Ericsson Patent Counsel

Date: March 4, 2010

Ericsson Inc.  
6300 Legacy Drive, M/S EVR1 C-11  
Plano, Texas 75024

(972) 583-5799  
roger.burleigh@ericsson.com

John Emery

## **CLAIMS APPENDIX**

1. (Currently Amended) A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of;

assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;

determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,

creating, at the first unit, the check token for the second unit based on the token secret and the password;

sending the check token to the second unit; and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit.

2. (Currently Amended) The method of claim 1, further comprising the step of: deleting the password and all significant parameters generated except the authentication tokens after usage thereof.

3. (Previously Presented) The method of claim 1, further comprising the step of: accepting, at the second unit, in response to a successful authentication, update information securely transferred from the first unit, at least a portion of the update information being created at the first unit.

4. (Previously Presented) The method of claim 3, wherein the update information is associated with revocation of a non-trusted group member.

5. (Previously Presented) The method of claim 3, wherein the update information relates to a password change.
6. (Currently Amended) The method of claim 3, wherein the update information is selected from the group consisting of:  
new authentication tokens,  
a new group key, a group-defining list, and,  
a revocation list, including combinations thereof.
7. (Previously Presented) The method of claim 3, further comprising the step of delegating update rights to a third intermediate unit, and sending at least a portion of the update information for the second unit to the intermediate unit.
8. (Previously Presented) The method of claim 7, wherein the update information is accompanied by a time stamp for determining whether the update information is still valid when the intermediate unit encounters the second unit.
9. (Previously Presented) The method of claim 7, wherein the delegation of update rights comprises delegation of rights to further delegate update rights.
10. (Previously Presented) The method of claim 1, wherein the assigning step further comprises the steps of;  
determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; and,  
creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password.
11. (Previously Presented) The method of claim 10 wherein the step of determining the token secret involves generating the token secret, as a part of an initial set-up procedure.

12. (Cancelled).
13. (Currently Amended) The method of claim 10, wherein the creating step involves using a bijective locking function having input parameters which include the token secret and a one-way function of the password.
14. (Previously Presented) The method of claim 13, wherein the locking function is a symmetric encryption function.
15. (Previously Presented) The method of claim 13, wherein the locking function is implemented through password-based secret sharing.
16. (Currently Amended) The method of claim 1, further comprising policies in at least one of the units in the group for limiting a number and/or frequency of authentication attempts.
17. (Currently Amended) The method of claim 1, further comprising the step of generating an alarm signal if a number of authentication attempts exceeds a predetermined value.
18. (Currently Amended) The method of claim 1, further comprising the step of sending an authentication response message from the second unit indicating a result of the comparing step.
19. (Previously Presented) The method of claim 1, further comprising the step of authentication of the second unit towards the first unit, whereby the first and second units are mutually authenticated towards each other.
20. (Previously Presented) The method of claim 19, further comprising the steps of:



generating a respective random value at the first and second unit;  
determining temporary test secrets at the first and second unit based on the random values; and,  
exchanging the temporary test secrets between the first and second unit for mutual authentication purposes.

21. (Previously Presented) The method of claim 1, wherein critical operations for which authentication is needed are listed in policies in at least one of the units.

22. (Previously Presented) The method of claim 3, wherein a unit that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units.

23. (Previously Presented) The method of claim 1, wherein the group of units constitutes a Personal Area Network (PAN).

24. (Previously Presented) The method of claim 1, wherein the authentication tokens are tamper-resistantly stored in the respective units.

25. (Currently Amended) A communication system including a group of at least two units associated with a common password, and means for password-based authentication, comprising:

means for assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining, at a first unit, a check token for a second unit based on the password and the authentication token of the first unit; and

means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit;

wherein the means for determining the check token comprises:

means for retrieving, at the first unit, a token secret using the authentication token of the first unit and the password; and,

means for creating, at the first unit, the check token for the second unit based on the token secret and the password.

26. (Currently Amended) The system of claim 25, further comprising means for deleting the password and parameters generated except the authentication tokens after usage thereof.

27. (Previously Presented) The system of claim 25, further comprising;  
means for transferring update information from the first unit to the second unit;  
and,  
means for accepting, at the second unit, update information from the first unit in response to a successful authentication.

28. (Previously Presented) The system of claim 27, wherein the update information is associated with revocation of a non-trusted group member.

29. (Previously Presented) The system of claim 27, wherein the update information relates to a password change.

30. (Currently Amended) The system of claim 27, wherein the update information is selected from the group consisting of new authentication tokens, a new group key, a group-defining list, and a revocation list, including combinations thereof.

31. (Previously Presented) The system of claim 27, further comprising means for delegation of update rights to a third intermediate unit, and means for sending at least a portion of the update information for the second unit to the intermediate unit.

32. (Previously Presented) The system of claim 25, wherein the means for assigning further comprises;

means for determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; and,

means for creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password.

33. (Cancelled).

34. (Currently Amended) The system of claim 32, wherein the means for creating involves a bijective locking function having input parameters which include the token secret and a one-way function of the password.

35. (Currently Amended) The system of claim 25, further comprises policies implemented in at least one of the units in the group for limiting a number and/or frequency of authentication attempts.

36. (Currently Amended) The system of claim 25, further comprising means for generating an alarm signal if a number of authentication attempts exceeds a predetermined value.

37. (Previously Presented) The system of claim 25, further comprising means for sending an authentication response message from the second unit.

38. (Previously Presented) The system of claim 25, further comprising means for mutual authentication between two units in the group.

39. (Previously Presented) The system of claim 25, wherein policies defining critical operations for which authentication is needed.

40. (Previously Presented) The system of claim 25, wherein said communication system being a Personal Area Network (PAN).

41. (Currently Amended) A first device belonging to a group of at least two devices associated with a common password, and including means for password-based authentication, the first device comprises:

means for receiving a password; means for assigning individual authentication tokens to other devices in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining a check token for a second device in the group based on the password and the authentication token of the first device; and

means for transmitting the check token to the second device for authentication towards the second device;

wherein the means for determining the check token comprises:

means for retrieving a token secret using the authentication token of the first device and the password; and,

means for creating the check token for the second device based on the token secret and the password.

42. (Currently Amended) The device of claim 41, further comprising means for deleting the password and parameters generated except the authentication token after usage thereof.

43. (Previously Presented) The device of claim 41, further comprising;  
means for creating update information for the second device; and,  
means for securely transferring update information to the second device.

44. (Previously Presented) The device of claim 43, further comprising means for delegation of update rights to an intermediate device, and means for sending update information for the second device to the intermediate device.

45. (Previously Presented) The device of claim 41, wherein the means for assigning further comprises;

means for determining a token secret common for the group and non-correlated with the password; and,

means for creating the authentication token for another device in the group based on the token secret and the password.

46-47. (Cancelled).

\* \* \*

**EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

None.